UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON AT TACOMA

Alicia LeDuc Montgomery, individually and on behalf of all others similarly situated, Plaintiff, v. AT&T, Inc., Defendant.	No. CLASS ACTION COMPLAINT

1. Plaintiff Alicia LeDuc Montgomery brings this action against Defendant AT&T, Inc. ("Defendant" or "AT&T") on behalf of the victims of a targeted cyberattack on AT&T that was announced on July 12, 2024 ("the Data Breach"). Plaintiff brings this action against Defendant for its failure to properly secure and safeguard the sensitive personal information of herself and all those similarly situated, and, in compensation for that failure, she seeks monetary damages, restitution, and/or injunctive relief. The following allegations are made upon information and belief derived from, among other things, investigation of counsel, public sources, and the facts and circumstances as currently known. Because only AT&T (as well as the cybercriminals who perpetrated the Data Breach) have knowledge of what information was compromised, Plaintiff reserves the right to supplement these allegations with additional facts and injuries as they are discovered.

KELLER ROHRBACK L.L.P.
1201 Third Avenue, Suite 3400
Seattle, WA 98101-3268
TELEPHONE: (206) 623-1900
FACSIMILE: (206) 623-3384

I. JURISDICTION AND VENUE

2. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(d)(2), because this is a class action in which the matter in controversy exceeds the sum of $5,000,000, there are more than 100 proposed Class Members, and minimal diversity exists, as Defendant is a citizen of States different from that of at least one Class member. This Court also has supplemental jurisdiction pursuant to 28 U.S.C. § 1367(a) because all claims alleged herein form part of the same case or controversy.

3. This Court has personal jurisdiction over Defendant because AT&T is authorized to and regularly conducts business in the State of Washington, including by selling, marketing, and advertising its products and services to Class Members located in the State of Washington and within this District. Defendant therefore has sufficient minimum contacts to render the exercise of jurisdiction by this Court proper and necessary.

4. Venue is proper in this District pursuant to 28 U.S.C. § 1391 because a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in this District.

II. PARTIES

5. Plaintiff Alicia LeDuc Montgomery is an individual resident of the State of Washington and a customer of AT&T.

6. Defendant AT&T, Inc. is a corporation organized under the state laws of Delaware with its principal place of business located in Dallas, Texas. It is one of the largest wireless carriers in the country.

III. FACTUAL ALLEGATIONS

7. In the course of their relationship, consumers, including Plaintiff and Class Members, provided Defendant with personally identifiable information, including their names, dates of birth, phone numbers, Social Security numbers, and other sensitive information.

8. Upon information and belief, in the course of collecting personally identifying information from consumers, including Plaintiff, Defendant promised to provide confidentiality

KELLER ROHRBACK L.L.P.
1201 Third Avenue, Suite 3400
Seattle, WA 98101-3268
TELEPHONE: (206) 623-1900
FACSIMILE: (206) 623-3384

and adequate security for the data it collected from consumers through its applicable privacy policy and through other disclosures in compliance with statutory privacy requirements.

9. For instance, Defendant's Privacy Notice provides:

> We work hard to safeguard your information using technology controls and organizational controls. We protect our computer storage and network equipment. We require employees to authenticate themselves to access sensitive data. We limit access to personal information to the people who need access for their jobs. And we require callers and online users to authenticate themselves before we provide account information.[1]

10. Defendant also provides on its website that:

> As the digital landscape grows, our employees, customers and partners depend on us to help protect them from cyberattacks. AT&T operates one of the world's most advanced and powerful global backbone networks and is a recognized leading provider of IP-based communication services. We have a responsibility to safeguard customer information. Security is at the core of our network and central to everything we do.
>
> We regularly evaluate and deploy new tools and systems that deliver highly effective safeguards against attempted cyberattacks. We also invest in customer solutions and trainings to raise awareness of customers' agency in protecting themselves from fraud.[2]

11. Defendant further provides on its website that:

> AT&T uses a consistent, disciplined global process to promptly identify security incidents and threats, minimize the loss or compromise of information, and facilitate incident resolution. AT&T maintains 24/7, near-real-time security monitoring of the AT&T network for investigation, action and response to network security events. Our threat management platform and program provide near-real-time data correlation, situational awareness reporting, active incident investigation, case management, trending analysis and predictive security alerting.

[1] AT&T, Inc., *AT&T Privacy Notice* (July 17, 2024), https://about.att.com/privacy/privacy-notice.html.

[2] AT&T, Inc., *Network & Data Security*, https://sustainability.att.com/priority-topics/network-data-security (last visited July 18, 2024).

KELLER ROHRBACK L.L.P.
1201 Third Avenue, Suite 3400
Seattle, WA 98101-3268
TELEPHONE: (206) 623-1900
FACSIMILE: (206) 623-3384

> AT&T uses the same set of security tools to manage our global network that we use for enterprise customers.[3]

12. Plaintiff and the Class Members relied on these promises and on this sophisticated business entity to keep their sensitive personally identifiable information confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information. Consumers, in general, demand security to safeguard their personally identifiable information.

A. The Data Breach

13. In April 2024, AT&T became aware that a third party or third parties accessed and captured the call logs of more than 100 million AT&T wireless customers. The call log information contains the records of calls and text messages, from the six months between May 1, 2022 and October 31, 2022, as well as on January 2, 2023. Because the information identifies each telephone number that an AT&T cellular number interacted with during the time period, it also includes the records of consumers who receive their phone service from carriers other than AT&T (the "Call Log Information").

14. The Call Log Information comprises an array of highly personal information, including the phone number of the AT&T customer, the phone numbers that the AT&T customer called or texted, the number of times the AT&T customer interacted with each phone number, and call durations ("Personal Information"). Many records also included information about the AT&T customers' locations, in the form of cell site ID numbers.

15. AT&T had uploaded the Call Log Information to the servers of a third party called Snowflake, a company that provides cloud-storage services, effectively outsourcing its responsibility to guard the consumer information that was ultimately stolen by hackers.

16. Shockingly, AT&T's account on Snowflake could be accessed simply through a username and password. Multi-factor authentication was not required.

[3] *Id.*

KELLER ROHRBACK L.L.P.
1201 Third Avenue, Suite 3400
Seattle, WA 98101-3268
TELEPHONE: (206) 623-1900
FACSIMILE: (206) 623-3384

17. Even more shockingly, ***Snowflake made multi-factor authentication available to its corporate customers—AT&T just decided not to use it.***

18. The Data Breach here was not the only recent theft of personally identifiable information stored on Snowflake. Other companies, including Ticketmaster, QuoteWizard, Santander, LendingTree, and Advance Auto Parts, have recently confirmed that they had customer data stolen from Snowflake.

B. AT&T's failure to responsibly protect consumers' personally identifiable information

19. The Data Breach is attributable to AT&T's failure to comply with state and federal laws and requirements as well as industry standards governing the protection of personally identifiable information.

20. For example, at least 24 states have enacted laws addressing data security practices that require that businesses that own, license or maintain personally identifiable information to implement and maintain "reasonable security procedures and practices" and to protect personally identifiable information from unauthorized access. California is one such state, which requires that "[a] business that owns, licenses, or maintains personal information about a California resident shall implement and maintain reasonable security procedures appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use modification or disclosure." Cal. Civ. Code § 1798.81.5(b).

21. AT&T also failed to comply with Federal Trade Commission ("FTC") guidance on protecting personally identifiable information and industry-standard cybersecurity practices. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce," including, as interpreted by the FTC, a failure by a company like Defendant to use reasonable measures to protect personally identifiable information. Several publications by the FTC outline the importance of implementing reasonable security systems to protect data. The FTC has made clear that protecting sensitive consumer data should factor into virtually all

KELLER ROHRBACK L.L.P.
1201 Third Avenue, Suite 3400
Seattle, WA 98101-3268
TELEPHONE: (206) 623-1900
FACSIMILE: (206) 623-3384

business decisions.

22. The FTC recommends, among other things:

a. limiting access to consumer information to those who have a legitimate business need for it;

b. encrypting consumer information on system and in transit;

c. implementing multi-factor authentication for anyone accessing consumer information;

d. implementing procedures and controls to monitor when authorized users are accessing consumer information;

e. maintaining up-to-date and appropriate programs and controls to prevent unauthorized access to consumer information; and

f. implementing procedures and controls to detect unauthorized access to consumer information, including monitoring activity logs for signs of unauthorized access to consumer information.

23. The FTC has also issued numerous guides for businesses highlighting the importance of reasonable data security practices.

24. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business.[4] The guidelines note businesses should protect the personal consumer information that they keep; properly dispose of personally identifiable information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems. The guidelines also recommend that businesses use an intrusion-detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the

[4] Fed. Trade Comm'n, *Protecting Personal Information: A Guide for Business* (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

KELLER ROHRBACK L.L.P.
1201 Third Avenue, Suite 3400
Seattle, WA 98101-3268
TELEPHONE: (206) 623-1900
FACSIMILE: (206) 623-3384

system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

25. The FTC recommends that businesses delete payment card information after the time needed to process a transaction; restrict employee access to sensitive consumer information; require strong passwords be used by employees with access to sensitive consumer information; apply security measures that have proven successful in the particular industry; and verify that third parties with access to sensitive information use reasonable security measures.

26. The FTC also recommends that companies use an intrusion detection system to immediately expose a data breach; monitor incoming traffic for suspicious activity that indicates a hacker is trying to penetrate the system; monitor for the transmission of large amounts of data from the system; and develop a plan to respond effectively to a data breach in the event one occurs.

27. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect consumer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

28. The FTC has interpreted Section 5 of the FTC Act to encompass failures to appropriately store and maintain personal data.

29. AT&T was aware of its obligations to protect consumers' personally identifiable information and privacy before and during the Data Breach yet failed to take reasonable steps to protect consumers' information from unauthorized access. It was also aware of the significant repercussions if it failed to do so because AT&T collected personally identifiable information from millions of consumers and it knew that this PII, if hacked, would result in injury to consumers, including Plaintiff and Class Members. In fact, AT&T should have been particularly aware of its obligations and the potential repercussions of not fulling those obligations as it had

KELLER ROHRBACK L.L.P.
1201 Third Avenue, Suite 3400
Seattle, WA 98101-3268
TELEPHONE: (206) 623-1900
FACSIMILE: (206) 623-3384

an extremely recent and massive data breach in March 2024 involving the PII of 73 million of AT&T's current and former customers.

C. Injuries to Plaintiff and Class Members

30. The collection of personally identifiable information of consumers that has now been stolen, even without the content of calls and texts, enables third parties to identify individual persons and uncover otherwise private (and extremely sensitive) information about them. As AT&T has acknowledged in response to the Data Breach, "there are often ways, using publicly available online tools, to find the name associated with a specific telephone number."[5]

31. Consider a 2016 study authored by computer scientists from Stanford University.[6] These scientists, using telephone metadata of the kind that was accessed in the Data Breach, were able to find out a great deal about the telephone users. Through manual and automated searches on the internet, they identified 82% of the users' names. They also were able to uncover the names of businesses users had called; when plotted on a map, they typically clustered so as to reveal where the telephone user likely lived. Indeed, the scientists were nearly 90% accurate in placing users within 50 miles of their home. Note, too, that these statistics almost certainly understate the extent to which telephone metadata can reveal names and locations, since the scientists used free public interfaces on the internet, rather than commercial databases.

32. In this same study, the authors discussed how they were able to infer extremely sensitive information about the telephone users. The metadata allowed the scientists to infer that one person had a serious heart condition, that another owned a rifle, that another had multiple sclerosis and that still another had just become pregnant.

33. Knowledge of a person's physical location, contact habits, and telephone number also enables a wide range of fraud and other harm. For example, once a fraudster figures out that

[5] AT&T, *AT&T Addresses Illegal Download of Customer Data* (July 12, 2024), https://about.att.com/story/2024/addressing-illegal-download.html.

[6] Jonathan Meyer et al., *Evaluating the Privacy Properties of Telephone Metadata*, PNAS (May 16, 2016), https://www.pnas.org/doi/full/10.1073/pnas.1508081113.

KELLER ROHRBACK L.L.P.
1201 Third Avenue, Suite 3400
Seattle, WA 98101-3268
TELEPHONE: (206) 623-1900
FACSIMILE: (206) 623-3384

a telephone user banks at Wells Fargo, it is easier to pose as Wells Fargo in a fraudulent telephone call or text. This is just one example, however, and the potential permutations of such attempts at fraud are endless. Under any permutation, however, those whose Personal Information has been accessed in the Data Breach are harmed: a malicious actor credibly poses as a trusted third party, the individual discloses further sensitive information to the malicious actor, and the malicious actor uses that information to do harm.

34. Further, malicious actors often wait months or years to use the information obtained in data breaches, as victims often become complacent and less diligent in monitoring their accounts after a significant period has passed. These bad actors will also re-use stolen information, meaning individuals can be the victim of several instances of identity theft, fraud, or other cybercrimes stemming from a single data breach.

35. The U.S. Government Accountability Office determined that "stolen data may be held for up to a year or more before being used to commit identity theft," and that "once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years." Moreover, there is often significant lag time between when a person suffers harm due to theft of their personally identifiable information and when they discover the harm. Plaintiff will therefore need to spend time and money to continuously monitor her accounts for years to ensure her personally identifiable information obtained in the Data Breach is not used to harm her. Plaintiff and Class Members thus have been harmed in the amount of the actuarial present value of ongoing high-quality identity defense and credit monitoring services made necessary as mitigation measures because of the Data Breach. In other words, Plaintiff has been harmed by the value of identity protection services she must purchase in the future to ameliorate the risk of harm she now faces due to the Data Breach.

36. Reporting on the Data Breach provides additional specifics. According to an article in Wired, which is based on communications with the security researcher who disclosed the breach to AT&T and was in contact with the hacker, the hacker who accessed the AT&T data

KELLER ROHRBACK L.L.P.
1201 Third Avenue, Suite 3400
Seattle, WA 98101-3268
TELEPHONE: (206) 623-1900
FACSIMILE: (206) 623-3384

"demonstrated how easily he could identify the owners of the numbers using a reverse-lookup program that identified by name the family members, colleagues, and others attached to the phone numbers who communicated with them."[7]

37. Though the security researcher believes that the hacker has deleted the data, he is not sure how many people received or otherwise accessed the data between the time the hacker stole it and when he deleted it.[8] There is no way to determine whether anyone who received or accessed the data before it was taken down has made it available to or otherwise disseminated it to others, and no way to track down and confirm the deletion of any such information.

38. Thus, the risk of these harms is ongoing, and Plaintiff and Class Members continue to be at an imminent risk of suffering future damages associated with the unauthorized use and misuse of their information, as there is an ongoing risk that data thieves and malicious actors who accessed the stolen information will use the information to the detriment of Plaintiff and Class Members for many years to come.

39. As a direct result of the Data Breach, Plaintiff and Class Members have suffered actual and/or attempted identity theft and fraud, and they will continue to be exposed to a heightened and imminent risk of identity theft and fraud, potentially for the rest of their lives. Plaintiff and Class Members must now and in the future closely monitor their medical, insurance, and financial accounts to guard against identity theft and fraud.

40. For this reason, Class Members may incur out-of-pocket costs for purchasing protective measures to deter and detect identity theft and fraud, as well as protective measures to mitigate against the misuse of their information.

41. As a direct and proximate result of the Data Breach and subsequent exposure of their personally identifiable information, Plaintiff and Class Members have suffered, and will continue to suffer, damages and economic losses in the form of lost time needed to take

[7] Kim Zetter, *AT&T Paid a Hacker $370,000 to Delete Stolen Phone Records*, Wired (July 14, 2024), https://www.wired.com/story/atandt-paid-hacker-300000-to-delete-stolen-call-records/.
[8] *Id.*

KELLER ROHRBACK L.L.P.
1201 Third Avenue, Suite 3400
Seattle, WA 98101-3268
TELEPHONE: (206) 623-1900
FACSIMILE: (206) 623-3384

appropriate measures to avoid the misuse of their information, potential unauthorized and fraudulent charges, and dealing with spam phone calls, letters, text messages, and emails received as a result of the Data Breach and the unauthorized disclosure and misuse of their personally identifiable information.

42. Plaintiff and Class Members have also realized harm in the lost or reduced value of their personally identifiable information. Plaintiff's personally identifiable information is not only valuable to AT&T, but Plaintiff also places high value on her personally identifiable information based on her understanding that it is a financial asset to companies that collect it.

43. Plaintiff and Class Members have also been harmed and damaged in the amount of the market value of the hacker's access to Plaintiff's information that was permitted without authorization by AT&T. This market value can be determined by reference to both legitimate and illegitimate markets for personally identifiable information.

44. Moreover, Plaintiff and Class Members value the privacy of this information and expect AT&T to allocate enough resources to ensure it is adequately protected. Plaintiff and other customers would not have done business with AT&T, provided their personally identifiable information, or paid the same prices for AT&T's goods and services had they known that AT&T did not implement reasonable security measures to protect their personally identifiable information. Customers reasonably expect that the payments they have made to AT&T incorporate the costs to implement reasonable security measures to protect their customers' information. As a result, Plaintiff and Class Members who are AT&T customers did not receive the benefit of their bargain with AT&T because they paid a value for services they expected but did not receive.

45. Given AT&T's failure to protect Plaintiff's and the Class Members' personally identifiable information, Plaintiff has a significant and cognizable interest in obtaining injunctive and equitable relief (in addition to any monetary damages, restitution, or disgorgement) that protects her from suffering further harm, as her personally identifiable information remains in

KELLER ROHRBACK L.L.P.
1201 Third Avenue, Suite 3400
Seattle, WA 98101-3268
TELEPHONE: (206) 623-1900
FACSIMILE: (206) 623-3384

AT&T's possession. Accordingly, this action represents the enforcement of an important right affecting the public interest and will confer a significant benefit on a large class of persons.

46. In sum, Plaintiff and Class Members were injured as follows: (i) theft of their personally identifiable information and the resulting loss of privacy rights in that information; (ii) improper disclosure of their personally identifiable information; (iii) loss of value of their personally identifiable information; (iv) the lost value of access to Plaintiff's and Class Members' personally identifiable information permitted by AT&T; (v) the amount of the actuarial present value of ongoing high-quality identity defense and credit monitoring services made necessary as mitigation measures because of the Data Breach; (vi) AT&T's retention of profits attributable to Plaintiff's and Class Members' personally identifiable information that AT&T failed to adequately protect; (vii) the certain, imminent, and ongoing threat of fraud and identity theft, including the economic and non-economic impacts that flow therefrom; (viii) ascertainable out-of-pocket expenses and the value of their time allocated to fixing or mitigating the effects of the Data Breach; (ix) overpayments to AT&T for services purchased, as Plaintiff and other AT&T customers reasonably believed a portion of the sale price would fund reasonable security measures that would protect her personally identifiable information, which was not the case; and (x) nominal damages.

IV. CLASS ACTION ALLEGATIONS

A. Nationwide class

47. Pursuant to Fed. R. Civ. P. 23(b)(2) and (b)(3), as applicable, and (c)(4), Plaintiff seeks certification of the following nationwide class (the "Nationwide Class" or the "Class"):

> All natural persons residing in the United States whose personally identifiable information was exfiltrated in the Data Breach.

48. The Nationwide Class consists of Customers (those natural persons who have a customer relationship with AT&T) and Non-Customers (those natural persons who have no customer relationship with AT&T). The Nationwide Class asserts claims against AT&T for

KELLER ROHRBACK L.L.P.
1201 Third Avenue, Suite 3400
Seattle, WA 98101-3268
TELEPHONE: (206) 623-1900
FACSIMILE: (206) 623-3384

negligence (Count 1), negligence per se (Count 2), breach of implied contract (Count 3), unjust enrichment (Count 4), and declaratory judgment (Count 5). The Nationwide Class consisting of Customers additionally alleges breach of express contract (Count 6).

B. Washington subclass

49. Pursuant to Fed. R. Civ. P. 23(b)(2) and (b)(3), as applicable, and (c)(4), Plaintiff seeks certification of a Washington Subclass in the alternative to the nationwide claims (Counts 1 through 6), as well as with respect to statutory claims under the Washington Data Breach Notice Act, Wash. Rev. Code §§ 19.255.010, et seq. (Count 6), and the Washington Consumer Protection Act, Wash. Rev. Code. Ann. §§ 19.86.020, et seq. (Count 7), on behalf of a Washington Subclass, defined as follows:

> All natural persons residing in Washington whose personally identifiable information was exfiltrated in the Data Breach.

50. Excluded from the Nationwide Class and the Washington Subclass (collectively, the "Class") are AT&T, any entity in which AT&T has a controlling interest, and AT&T's officers, directors, legal representatives, successors, subsidiaries, and assigns. Also excluded from the Class are any judicial officer presiding over this matter, members of their immediate family, and members of their judicial staff.

51. **Numerosity: Federal Rule of Civil Procedure 23(a)(1).** The members of the Nationwide Class and the Washington Subclass are so numerous and geographically dispersed that individual joinder of all Class Members is impracticable. While the exact number of Class Members is unknown to Plaintiff at this time, AT&T has acknowledged that millions of individuals' personally identifiable information has been compromised. The names, addresses, and phone numbers of such individuals who are AT&T customers are available from AT&T's records, and those Class Members may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods. On information and belief, information about such individuals who are not AT&T customers is also available, including through information

KELLER ROHRBACK L.L.P.
1201 Third Avenue, Suite 3400
Seattle, WA 98101-3268
TELEPHONE: (206) 623-1900
FACSIMILE: (206) 623-3384

compromised in the Data Breach, and those Class Members may also be notified of the pendency of this action by recognized, Court-approved notice dissemination methods. On information and belief, there are at least thousands of individuals in the Nationwide Class and at least thousands of individuals in the Washington Statewide Subclass, making joinder of all Class Members impracticable.

52. **Commonality and Predominance: Federal Rules of Civil Procedure 23(a)(2) and 23(b)(3).** As to both the Nationwide Class and the Washington Subclass, this action involves common questions of law and fact, which predominate over any questions affecting individual Class Members. The common questions include:

a. Whether AT&T had a duty to protect consumers' personally identifiable information;

b. Whether AT&T failed to take reasonable and prudent security measures to ensure the personally identifiable information of consumers that it collects and maintains was protected;

c. Whether AT&T failed to take available steps to prevent and stop the Data Breach from happening;

d. Whether AT&T knew or should have known that the personally identifiable information it maintains was vulnerable to compromise;

e. Whether AT&T was negligent in failing to implement reasonable and adequate security procedures and practices;

f. Whether AT&T's security measures to protect the personally identifiable information it maintains were reasonable in light known legal requirements;

g. Whether AT&T's conduct constituted unfair or deceptive trade practices;

h. Whether AT&T violated state or federal law when it failed to implement reasonable security procedures and practices;

i. Which security procedures and notification procedures AT&T should be required

KELLER ROHRBACK L.L.P.
1201 Third Avenue, Suite 3400
Seattle, WA 98101-3268
TELEPHONE: (206) 623-1900
FACSIMILE: (206) 623-3384

to implement;

j. Whether AT&T has a contractual obligation to provide for the security of consumer personally identifiable information;

k. Whether AT&T has complied with any contractual obligations to protect consumer personally identifiable information;

l. Whether AT&T had any contractual obligations or other duties to provide for the security of personally identifiable information of individuals who are not its customers, but who communicate with its customers;

m. What security measures, if any, must be implemented by AT&T to comply with its contractual obligations or other duties;

n. Whether AT&T violated state consumer protection laws in connection with the actions described herein;

o. Whether AT&T failed to notify Plaintiff and Class Members as soon as practicable and without delay after the Data Breach was discovered;

p. Whether AT&T's conduct resulted in or was the proximate cause of the loss of the personally identifiable information of Plaintiff and Class Members;

q. Whether Plaintiff and Class Members were injured and suffered damages or other losses because of AT&T's failure to reasonably protect their personally identifiable information;

r. Whether AT&T should retain the money paid by Plaintiff and Class Members to protect their personally identifiable information, and the profits AT&T generated through Plaintiff's and Class Members' personally identifiable information;

s. Whether and how AT&T should retain Plaintiff's and Class Members' valuable personally identifiable information; and,

t. Whether Plaintiff and Class Members are entitled to damages or injunctive relief.

53. **Typicality: Federal Rule of Civil Procedure 23(a)(3).** As to the Nationwide

KELLER ROHRBACK L.L.P.
1201 Third Avenue, Suite 3400
Seattle, WA 98101-3268
TELEPHONE: (206) 623-1900
FACSIMILE: (206) 623-3384

Class and the Washington Subclass, Plaintiff's claims are typical of other Class Members' claims because Plaintiff and Class Members were subjected to the same allegedly unlawful conduct and damaged in the same way. Plaintiff's personally identifiable information was in AT&T's possession at the time of the Data Breach and was compromised as a result of the Data Breach. Plaintiff's damages and injuries are akin to those of other Class Members, and Plaintiff seeks relief consistent with the relief of the Class.

54. **Adequacy of Representation: Federal Rule of Civil Procedure 23(a)(4).** Consistent with Rule 23(a)(4), Plaintiff is an adequate representative of the Nationwide Class and the Washington Subclass because Plaintiff is a member of the Nationwide Class and the Washington Subclass and is committed to pursuing this matter against Defendant to obtain relief for the Class. Plaintiff has no conflicts of interest with the Class. Plaintiff's Counsel are competent and experienced in litigating class actions, including extensive experience in data breach and privacy litigation. Plaintiff intends to vigorously prosecute this case and will fairly and adequately protect the Class's interests.

55. **Predominance and Superiority: Federal Rule of Civil Procedure 23(b)(3).** Consistent with Rule 23(b)(3), a class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. Common issues in this litigation also predominate over individual issues because those issues discussed in the above paragraph on commonality are more important to the resolution of this litigation than any individual issues. The purpose of the class action mechanism is to permit litigation against wrongdoers even when damages to individual plaintiffs may not be sufficient to justify individual litigation. Here, the damages suffered by Plaintiff and the Class are relatively small compared to the burden and expense required to individually litigate their claims against AT&T, and thus, individual litigation to redress AT&T's wrongful conduct would be impracticable. Individual litigation by each Class Member would also strain the court system. Individual litigation creates the potential

KELLER ROHRBACK L.L.P.
1201 Third Avenue, Suite 3400
Seattle, WA 98101-3268
TELEPHONE: (206) 623-1900
FACSIMILE: (206) 623-3384

for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economies of scale, and comprehensive supervision by a single court.

56. **Risk of Prosecuting Separate Actions.** This case is appropriate for certification because prosecuting separate actions by individual proposed Class Members would create the risk of inconsistent adjudications and incompatible standards of conduct for AT&T or would be dispositive of the interests of members of the proposed Class.

57. **Ascertainability**. The Nationwide Class and Washington Subclass are defined by reference to objective criteria, and there is an administratively feasible mechanism to determine who fits within the Class. The Nationwide Class and Washington Subclass consist of individuals who provided their personally identifiable information to AT&T. Class Membership can be determined using AT&T's records and/or information compromised in the Data Breach.

58. **Injunctive and Declaratory Relief**. Class certification is also appropriate under Rule 23(b)(2) and (c). AT&T, through its uniform conduct, acted or refused to act on grounds generally applicable to the Class as a whole, making injunctive relief appropriate to the Class as a whole. Injunctive relief is necessary to uniformly protect the Class Members' data. Plaintiff seeks prospective injunctive relief as a wholly separate remedy from any monetary relief.

59. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein.

V. CLAIMS ON BEHALF OF THE NATIONWIDE CLASS

COUNT ONE — NEGLIGENCE

On Behalf of Plaintiff and the Nationwide Class, or Alternatively, on Behalf of Plaintiff and the Washington Subclass

60. Plaintiff repeats and realleges the allegations contained in the Statement of Facts

KELLER ROHRBACK L.L.P.
1201 Third Avenue, Suite 3400
Seattle, WA 98101-3268
TELEPHONE: (206) 623-1900
FACSIMILE: (206) 623-3384

as if fully set forth herein.

61. AT&T required Plaintiff and Class Members to submit sensitive Personal Information in order to obtain its services. Moreover, in the course of Plaintiff's and the Class Members' use of AT&T services, AT&T acquired additional sensitive Personal Information.

62. AT&T owed a duty to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting their Personal Information in its possession from being compromised, lost, stolen, accessed or misused by unauthorized persons. More specifically, this duty included, among other things: (a) designing, maintaining, and testing AT&T's security systems to ensure that Plaintiff's and Class Members' Personal Information in AT&T's possession was adequately secured and protected; (b) implementing processes to ensure that any third parties to which AT&T disclosed Plaintiff's and Class Members' Personal Information implemented, maintain, and tested security systems to ensure that the information was adequately secured and protected; (c) implementing and utilizing processes to ensure that the transfer of Plaintiff's and Class Members' Personal Information between AT&T and third parties was secured and protected; (d) implementing processes that would detect unauthorized access to the Personal Information it maintains in a timely manner; (e) timely acting upon warnings and alerts, including those generated by its own security systems, regarding unauthorized access to the Personal Information it maintains; and (f) maintaining data security measures consistent with industry standards.

63. AT&T duty to use reasonable care arose from several sources, including but not limited to those described herein.

64. AT&T had common law duties to prevent foreseeable harm to Plaintiff and the Class Members. These duties existed because Plaintiff and Class Members were the foreseeable and probable victims of any inadequate security practices. Not only was it foreseeable that Plaintiff and Class Members would be harmed by AT&T's failure to protect their Personal Information because hackers routinely attempt to steal such information and use it for nefarious

KELLER ROHRBACK L.L.P.
1201 Third Avenue, Suite 3400
Seattle, WA 98101-3268
TELEPHONE: (206) 623-1900
FACSIMILE: (206) 623-3384

purposes, AT&T knew that it was more likely than not Plaintiff and other Class Members would be harmed if it allowed such a breach.

65. AT&T's duty to use reasonable security measures also arose as a result of the special relationship that existed between AT&T, on the one hand, and Plaintiff and Class Members, on the other hand. The special relationship arose because Plaintiff and Class Members entrusted AT&T with sensitive Personal Information as part of the purchase of the services AT&T offers. AT&T alone could have ensured that its security systems and data storage architecture were sufficient to prevent or minimize the Data Breach.

66. AT&T's duty also arose under Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect Personal Information by companies such as AT&T. Various FTC publications and data security breach orders further form the basis of AT&T's duty. In addition, individual states have enacted statutes based upon the FTC Act that also created a duty.

67. AT&T's duty also arose from its superior position to protect against the harm suffered by Plaintiff and Class Members as a result of the AT&T Data Breach.

68. AT&T admits that it has a responsibility to protect the Personal Information with which it is entrusted.

69. AT&T knew or should have known that its data storage architecture was vulnerable to unauthorized access and targeting by cybercriminals for the purpose of stealing and misusing confidential Personal Information.

70. AT&T also had a duty to safeguard the Personal Information of Plaintiff and Class Members and to promptly notify them of a breach because of state laws and statutes that require AT&T to reasonably safeguard sensitive Personal Information, as detailed herein.

71. Timely, adequate notification was required, appropriate and necessary so that, among other things, Plaintiff and Class Members could take appropriate measures to freeze or

KELLER ROHRBACK L.L.P.
1201 Third Avenue, Suite 3400
Seattle, WA 98101-3268
TELEPHONE: (206) 623-1900
FACSIMILE: (206) 623-3384

lock their credit profiles, avoid or mitigate identity theft or fraud, cancel or change usernames and passwords on compromised accounts, monitor their account information and credit reports for fraudulent activity, obtain credit monitoring services, and take other steps to mitigate or ameliorate the damages caused by AT&T's misconduct.

72. AT&T breached the duties it owed to Plaintiff and Class Members described above and thus was negligent. AT&T breached these duties by, among other things, failing to: (a) exercise reasonable care and implement adequate security systems, protocols, and practices sufficient to protect the Personal Information of Plaintiff and Class Members; (b) detect the Data Breach while it was ongoing; (c) maintain security systems consistent with industry standards during the period of the Data Breach; (d) comply with regulations protecting the Personal Information at issue during the period of the Data Breach; and (e) disclose in a timely and adequate manner that Plaintiff's and the Class Members' Personal Information in AT&T's possession had been or was reasonably believed to have been, stolen or compromised.

73. But for AT&T's wrongful and negligent breach of its duties owed to Plaintiff and Class Members, their Personal Information would not have been compromised.

74. AT&T's failure to take proper security measures to protect the sensitive Personal Information of Plaintiff and Class Members created conditions conducive to a foreseeable, intentional act, namely the unauthorized access of Plaintiff's and Class Members' Personal Information.

75. Plaintiff and Class Members were foreseeable victims of AT&T's inadequate data security practices, and it was also foreseeable that AT&T's failure to provide timely and adequate notice of the Data Breach would result in injury to Plaintiff and Class Members as described in this Complaint.

76. As a direct and proximate result of AT&T's negligence, Plaintiff and Class Members have been injured and are entitled to damages in an amount to be proven at trial. Such injuries include one or more of the following: ongoing, imminent, and impending threat of

KELLER ROHRBACK L.L.P.
1201 Third Avenue, Suite 3400
Seattle, WA 98101-3268
TELEPHONE: (206) 623-1900
FACSIMILE: (206) 623-3384

identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen Personal Information; illegal sale of the compromised Personal Information on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach reviewing bank statements, credit card statements, and credit reports, among other related activities; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the Personal Information; the amount of the actuarial present value of ongoing high-quality identity defense and credit monitoring services made necessary as mitigation measures because of AT&T's Data Breach; lost benefit of their bargains and overcharges for services or products; nominal and general damages and other economic and non-economic harm.

COUNT TWO — NEGLIGENCE *PER SE*

On Behalf of Plaintiff and the Nationwide Class,
or Alternatively, on Behalf of Plaintiff and the Washington Subclass

77. Plaintiff repeats and realleges the allegations contained in the Statement of Facts as if fully set forth herein.

78. Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the Federal Trade Commission ("FTC"), the unfair act or practice by companies such as AT&T of failing to use reasonable measures to protect Personal Information.

79. The FTC publications and orders also form the basis of AT&T's duty.

80. AT&T violated Section 5 of the FTC Act by failing to use reasonable measures to protect Personal Information and not complying with applicable industry standards. AT&T's conduct was particularly unreasonable given the nature and amount of Personal Information it obtained, stored, and disseminated, the foreseeable consequences of a data breach involving the

KELLER ROHRBACK L.L.P.
1201 Third Avenue, Suite 3400
Seattle, WA 98101-3268
TELEPHONE: (206) 623-1900
FACSIMILE: (206) 623-3384

highly sensitive Personal Information it maintains, including specifically the damages that would result to Plaintiff and Class Members, and the obviousness of its failure to comply with applicable industry standards such as dual-factor authentication.

81. In addition, under state data security statutes, AT&T had a duty to implement and maintain reasonable security procedures and practices to safeguard Plaintiff's and Class Members' Personal Information.

82. AT&T's violation of Section 5 of the FTC Act (and similar state statutes) constitutes negligence per se.

83. Plaintiff and Class Members are consumers within the class of persons Section 5 of the FTC Act was intended to protect.

84. The harm that has occurred is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses that, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

85. AT&T breached its duties to Plaintiff and Class Members under the FTC Act and state data security statutes by failing to provide fair, reasonable, or adequate data security practices to safeguard Plaintiff's and Class Members' Personal Information.

86. Plaintiff and Class Members were foreseeable victims of AT&T's violations of the FTC Act and state data security statutes. AT&T knew or should have known that its failure to implement reasonable measures to protect and secure Plaintiff's and Class Members' Personal Information would cause damage to Plaintiff and Class Members.

87. But for AT&T's violation of the applicable laws and regulations, Plaintiff's and Class Members' Personal Information would not have been accessed by unauthorized parties.

88. As a direct and proximate result of AT&T's negligence per se, Plaintiff and Class Members have been injured and are entitled to damages in an amount to be proven at trial. Such injuries include one or more of the following: ongoing, imminent, certainly impending threat of

KELLER ROHRBACK L.L.P.
1201 Third Avenue, Suite 3400
Seattle, WA 98101-3268
TELEPHONE: (206) 623-1900
FACSIMILE: (206) 623-3384

identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen Personal Information; illegal sale of the compromised Personal Information on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach reviewing bank statements, credit card statements, and credit reports, among other related activities; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the Personal Information; lost value of access to their Personal Information permitted by AT&T; the amount of the actuarial present value of ongoing high-quality identity defense and credit monitoring services made necessary as mitigation measures because of AT&T's Data Breach; lost benefit of their bargains and overcharges for services or products; nominal and general damages; and other economic and non-economic harm.

COUNT THREE — BREACH OF IMPLIED CONTRACT

On Behalf of Plaintiff and the Nationwide Class, or Alternatively, on Behalf of Plaintiff and the Washington Subclass

89. Plaintiff repeats and realleges the allegations contained in the Statement of Facts as if fully set forth herein.

90. Plaintiff and Class Members entered into an implied contract with AT&T when they obtained services from AT&T, or otherwise provided Personal Information to AT&T.

91. As part of these transactions, AT&T agreed to safeguard and protect the Personal Information of Plaintiff and Class Members and to timely and accurately notify them if their Personal Information was breached or compromised.

92. Plaintiff and Class Members entered into the implied contracts with the reasonable expectation that AT&T's data security practices and policies were reasonable and consistent with legal requirements and industry standards. Plaintiff and Class Members believed

KELLER ROHRBACK L.L.P.
1201 Third Avenue, Suite 3400
Seattle, WA 98101-3268
TELEPHONE: (206) 623-1900
FACSIMILE: (206) 623-3384

that AT&T would use part of the monies paid to AT&T under the implied contracts or the monies obtained from the benefits derived from the Personal Information they provided to fund adequate and reasonable data security practices.

93. Plaintiff and Class Members would not have provided and entrusted their Personal Information to AT&T or would have paid less for AT&T products or services in the absence of the implied contract or implied terms between them and AT&T. The safeguarding of the Personal Information of Plaintiff and Class Members was critical to realize the intent of the parties.

94. Plaintiff and Class Members fully performed their obligations under the implied contracts with AT&T.

95. AT&T breached its implied contracts with Plaintiff and Class Members to protect their Personal Information when it (1) failed to take reasonable steps to use safe and secure systems to protect that information; and (2) disclosed that information to unauthorized third parties.

96. As a direct and proximate result of AT&T's breach of implied contract, Plaintiff and Class Members have been injured and are entitled to damages in an amount to be proven at trial. Such injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen Personal Information; illegal sale of the compromised Personal Information on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach reviewing bank statements, credit card statements, and credit reports, among other related activities; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the Personal Information; lost value of access to their Personal Information permitted by AT&T; the

KELLER ROHRBACK L.L.P.
1201 Third Avenue, Suite 3400
Seattle, WA 98101-3268
TELEPHONE: (206) 623-1900
FACSIMILE: (206) 623-3384

amount of the actuarial present value of ongoing high-quality identity defense and credit monitoring services made necessary as mitigation measures because of AT&T's Data Breach; lost benefit of their bargains and overcharges for services or products; nominal and general damages; and other economic and non-economic harm.

COUNT FOUR — UNJUST ENRICHMENT

On Behalf of Plaintiff and the Nationwide Class, or Alternatively, on Behalf of Plaintiff and the Washington Subclass

97. Plaintiff repeats and realleges the allegations contained in the Statement of Facts as if fully set forth herein.

98. Plaintiff and Class Members have an interest, both equitable and legal, in the Personal Information about them that was conferred upon, collected by, and maintained by AT&T and that was ultimately stolen in the AT&T Data Breach.

99. AT&T was benefitted by the conferral upon it of the Personal Information pertaining to Plaintiff and Class Members and by its ability to retain, use, and profit from that information. AT&T understood that it was in fact so benefitted.

100. AT&T also understood and appreciated that the Personal Information pertaining to Plaintiff and Class Members was private and confidential and its value depended upon AT&T maintaining the privacy and confidentiality of that Personal Information.

101. But for AT&T's willingness and commitment to maintain its privacy and confidentiality, that Personal Information would not have been transferred to and entrusted with AT&T.

102. Because of its use of Plaintiff's and Class Members' Personal Information, AT&T sold more services than it otherwise would have. AT&T was unjustly enriched by profiting from the additional services it was able to market, sell, and create to the detriment of Plaintiff and

KELLER ROHRBACK L.L.P.
1201 Third Avenue, Suite 3400
Seattle, WA 98101-3268
TELEPHONE: (206) 623-1900
FACSIMILE: (206) 623-3384

Class Members.

103. AT&T also benefitted through its unjust conduct by retaining money that it should have used to provide reasonable and adequate data security to protect Plaintiff's and Class Members' Personal Information.

104. AT&T also benefitted through its unjust conduct in the form of the profits it gained through the use of Plaintiff's and Class Members' Personal Information.

105. It is inequitable for AT&T to retain these benefits.

106. As a result of AT&T's wrongful conduct as alleged in this Complaint (including among things its failure to employ adequate data security measures, its continued maintenance and use of the Personal Information belonging to Plaintiff and Class Members without having adequate data security measures, and its other conduct facilitating the unauthorized disclosure of that Personal Information), AT&T has been unjustly enriched at the expense of, and to the detriment of, Plaintiff and Class Members.

107. AT&T's unjust enrichment is traceable to, and resulted directly and proximately from, the conduct alleged herein, including the compiling and use of Plaintiff's and Class Members' sensitive Personal Information, while at the same time failing to maintain that information secure from unauthorized access by hackers and identity thieves.

108. It is inequitable, unfair, and unjust for AT&T to retain these wrongfully obtained benefits. AT&T's retention of wrongfully obtained monies would violate fundamental principles of justice, equity, and good conscience.

109. The benefit conferred upon, received, and enjoyed by AT&T was not conferred officiously or gratuitously, and it would be inequitable, unfair, and unjust for AT&T to retain the benefit.

110. AT&T's defective security and its unfair and deceptive conduct have, among other things, caused Plaintiff and Class Members to unfairly incur substantial time and/or costs to mitigate and monitor the use of their Personal Information and has caused the Plaintiff and

KELLER ROHRBACK L.L.P.
1201 Third Avenue, Suite 3400
Seattle, WA 98101-3268
TELEPHONE: (206) 623-1900
FACSIMILE: (206) 623-3384

Class Members other damages as described herein.

111. Plaintiff and the Class Members have no adequate remedy at law.

112. AT&T is therefore liable to Plaintiff and Class Members for restitution or disgorgement in the amount of the benefit conferred on AT&T as a result of its wrongful conduct, including specifically: the value to AT&T of the Personal Information that was stolen in the Data Breach; the profits AT&T received and is receiving from the use of that information; the amounts that AT&T overcharged Plaintiff and Class Members for use of AT&T's products and services; and the amounts that AT&T should have spent to provide reasonable and adequate data security to protect Plaintiff's and Class Members' Personal Information.

COUNT FIVE — DECLARATORY JUDGMENT

On Behalf of Plaintiff and the Nationwide Class, or Alternatively, on Behalf of Plaintiff and the Washington Subclass

113. Plaintiff repeats and realleges the allegations contained in the Statement of Facts as if fully set forth herein.

114. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, et seq., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. The Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

115. An actual controversy has arisen in the wake of the AT&T Data Breach regarding its present and prospective common law and other duties to reasonably safeguard consumers' Personal Information and whether AT&T is currently maintaining data security measures adequate to protect Plaintiff and Class Members from further data breaches that compromise their Personal Information. Plaintiff continues to suffer injury as a result of the compromise of Plaintiff's Personal Information and remain at imminent risk that further compromises of her Personal Information will occur in the future given the publicity around the Data Breach and the nature and quantity of the Personal Information stored by AT&T.

KELLER ROHRBACK L.L.P.
1201 Third Avenue, Suite 3400
Seattle, WA 98101-3268
TELEPHONE: (206) 623-1900
FACSIMILE: (206) 623-3384

116. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. AT&T continues to owe a legal duty to secure consumers' Personal Information and to timely notify consumers of a data breach under the common law, Section 5 of the FTC Act, and various state statutes;

b. AT&T continues to breach this legal duty by failing to employ reasonable measures to secure consumers' Personal Information.

117. The Court also should issue corresponding prospective injunctive relief requiring AT&T to employ adequate security protocols consistent with law and industry standards to protect consumers' Personal Information.

118. If an injunction is not issued, Plaintiff will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at AT&T. The risk of another such breach is real, immediate, and substantial. If another breach at AT&T occurs, Plaintiff will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and Plaintiff will be forced to bring multiple lawsuits to rectify the same conduct.

119. The hardship to Plaintiff if an injunction does not issue exceeds the hardship to AT&T if an injunction is issued. Among other things, if another significant data breach occurs at AT&T, Plaintiff will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to AT&T of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and AT&T has a pre-existing legal obligation to employ such measures.

120. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at AT&T, thus eliminating the additional injuries that would result to Plaintiff and the millions of consumers whose confidential information would be further compromised.

KELLER ROHRBACK L.L.P.
1201 Third Avenue, Suite 3400
Seattle, WA 98101-3268
TELEPHONE: (206) 623-1900
FACSIMILE: (206) 623-3384

COUNT SIX — BREACH OF EXPRESS CONTRACT

On Behalf of Plaintiff and the Nationwide Class, or Alternatively, on Behalf of Plaintiff and the Washington Subclass

121. Plaintiff repeats and realleges the allegations contained in the Statement of Facts as if fully set forth herein. For the purposes of this claim, Plaintiffs and Class Members shall mean natural persons who have a customer relationship with AT&T.

122. AT&T's Privacy Notice is an agreement between T-Mobile and individuals who provided their PII to T-Mobile, including Plaintiffs and Class Members.

123. AT&T's Privacy Notice states that it "explains how we use your information and keep it safe."

124. AT&T's Privacy Notice stated at the time of the Data Breach that:

> We work hard to safeguard your information using technology controls and organizational controls. We protect our computer storage and network equipment. We require employees to authenticate themselves to access sensitive data. We limit access to personal information to the people who need access for their jobs. And we require callers and online users to authenticate themselves before we provide account information.[9]

125. AT&T also acknowledged that, "[a]s the digital landscape grows, our employees, customers and partners depend on us to help protect them from cyberattacks," and that "[w]e have a responsibility to safeguard customer information."[10]

126. For this reason, AT&T represented that "[s]ecurity is at the core of our network and central to everything we do," and that "[w]e regularly evaluate and deploy new tools and systems that deliver highly effective safeguards against attempted cyberattacks," and "[w]e also invest in customer solutions and trainings to raise awareness of customers' agency in protecting

[9] AT&T, Inc., *AT&T Privacy Notice* (July 17, 2024), https://about.att.com/privacy/privacy-notice.html.

[10] AT&T, Inc., *Network & Data Security*, https://sustainability.att.com/priority-topics/network-data-security (last visited July 18, 2024).

KELLER ROHRBACK L.L.P.
1201 Third Avenue, Suite 3400
Seattle, WA 98101-3268
TELEPHONE: (206) 623-1900
FACSIMILE: (206) 623-3384

themselves from fraud."[11]

127. Likewise, AT&T represented to customers that:

> AT&T uses a consistent, disciplined global process to promptly identify security incidents and threats, minimize the loss or compromise of information, and facilitate incident resolution. AT&T maintains 24/7, near-real-time security monitoring of the AT&T network for investigation, action and response to network security events. Our threat management platform and program provide near-real-time data correlation, situational awareness reporting, active incident investigation, case management, trending analysis and predictive security alerting. AT&T uses the same set of security tools to manage our global network that we use for enterprise customers.[12]

128. Plaintiff and Class Members on the one side and AT&T on the other formed a contract when Plaintiff and Class Members obtained products or services from AT&T, or otherwise provided PII to AT&T subject to its Privacy Notice.

129. Plaintiff and Class Members fully performed their obligations under the contracts with AT&T.

130. AT&T breached its agreement with Plaintiff and Class Members by failing to protect their PII. Specifically, it (1) failed to take reasonable steps to use safe and secure systems to protect that information; and (2) disclosed that information to unauthorized third parties, in violation of the agreement.

131. As a direct and proximate result of AT&T's breach of contract, Plaintiff and Class Members have been injured and are entitled to damages in an amount to be proven at trial. Such injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen Personal Information; illegal sale of the compromised Personal Information on the black market; mitigation expenses

[11] *Id.*
[12] *Id.*

KELLER ROHRBACK L.L.P.
1201 Third Avenue, Suite 3400
Seattle, WA 98101-3268
TELEPHONE: (206) 623-1900
FACSIMILE: (206) 623-3384

and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach reviewing bank statements, credit card statements, and credit reports, among other related activities; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the Personal Information; lost value of access to their Personal Information permitted by AT&T; the amount of the actuarial present value of ongoing high-quality identity defense and credit monitoring services made necessary as mitigation measures because of AT&T's Data Breach; lost benefit of their bargains and overcharges for services or products; nominal and general damages; and other economic and non-economic harm.

VI. CLAIMS ON BEHALF OF THE WASHINGTON SUBCLASS

COUNT SEVEN — VIOLATION OF THE WASHINGTON DATA BREACH NOTICE ACT, WASH. REV. CODE §§ 19.255.010, ET SEQ.

On Behalf of Plaintiff and the Washington Subclass

132. Plaintiff, individually and on behalf of the Washington Subclass, incorporates all foregoing factual allegations as if fully set forth herein. This claim is brought individually under the laws of Washington and on behalf of all other natural persons whose Personal Information was compromised as a result of the Data Breach.

133. AT&T is a business that owns or licenses computerized data that includes "personal information" as defined by Wash. Rev. Code § 19.255.010(1).

134. Plaintiff's and Class Members' Personal Information includes "personal information" as covered under Wash. Rev. Code § 19.255.010(5).

135. AT&T is required to accurately notify Plaintiff and Class Members following discovery or notification of the breach of its data security program if Personal Information was, or is reasonably believed to have been, acquired by an unauthorized person and the Personal Information was not secured, in the most expedient time possible and without unreasonable delay under Wash. Rev. Code § 19.255.010(1).

KELLER ROHRBACK L.L.P.
1201 Third Avenue, Suite 3400
Seattle, WA 98101-3268
TELEPHONE: (206) 623-1900
FACSIMILE: (206) 623-3384

136. Because AT&T discovered a breach of its security system in which Personal Information was, or is reasonably believed to have been, acquired by an unauthorized person and the Personal Information was not secured, AT&T had an obligation to disclose the data breach in a timely and accurate fashion as mandated by Wash. Rev. Code § 19.255.010(1).

137. By failing to disclose the Data Breach to Plaintiff and all Class Members in a timely and accurate manner, AT&T violated Wash. Rev. Code § 19.255.010(1).

138. As a direct and proximate result of AT&T's violations of Wash. Rev. Code § 19.255.010(1), Plaintiff and Class Members suffered damages, as described above.

139. Plaintiff and Class Members seek relief under Wash. Rev. Code §§ 19.255.040, including actual damages and injunctive relief.

COUNT EIGHT — VIOLATION OF THE WASHINGTON CONSUMER PROTECTION ACT, WASH. REV. CODE ANN. §§ 19.86.020, ET SEQ.

On Behalf of Plaintiff and the Washington Subclass

140. Plaintiff, individually and on behalf of the Washington Subclass, incorporates all foregoing factual allegations as if fully set forth herein. This claim is brought individually under the laws of Washington and on behalf of all other natural persons whose Personal Information was compromised as a result of the Data Breach.

141. AT&T is a "person," as defined by Wash. Rev. Code Ann. § 19.86.010(1).

142. AT&T advertised, offered, or sold goods or services in Washington and engaged in trade or commerce directly or indirectly affecting the people of Washington, as defined by Wash. Rev. Code Ann. § 19.86.010 (2).

143. AT&T engaged in unfair or deceptive acts or practices in the conduct of trade or commerce, in violation of Wash. Rev. Code Ann. § 19.86.020, including:

A. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Class Members' Personal Information, which was a direct and proximate cause of the Data Breach;

KELLER ROHRBACK L.L.P.
1201 Third Avenue, Suite 3400
Seattle, WA 98101-3268
TELEPHONE: (206) 623-1900
FACSIMILE: (206) 623-3384

B. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

C. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class Members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

D. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Class Members' Personal Information, including by implementing and maintaining reasonable security measures;

E. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class Members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

F. Failing to timely and adequately notify Plaintiff and Class Members of the Data Breach;

G. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and Class Members' Personal Information; and

H. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class Members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

144. AT&T's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of AT&T's data security and ability to protect the confidentiality of consumers' Personal Information.

145. AT&T's representations and omissions were material because they were likely to

KELLER ROHRBACK L.L.P.
1201 Third Avenue, Suite 3400
Seattle, WA 98101-3268
TELEPHONE: (206) 623-1900
FACSIMILE: (206) 623-3384

deceive reasonable consumers, including Plaintiff and the Class Members, that their Personal Information was not exposed and misled Plaintiff and the Class Members into believing they did not need to take actions to secure their identities.

146. AT&T acted intentionally, knowingly, and maliciously to violate Washington's Consumer Protection Act, and recklessly disregarded Plaintiff's and Class Members' rights.

147. AT&T's conduct is injurious to the public interest because it violates Wash. Rev. Code Ann. § 19.86.020, violates a statute that contains a specific legislation declaration of public interest impact, including, but not limited to Wash. Rev. Code §§ 19.255.010, et seq. Alternatively, AT&T's conduct is injurious to the public interest because it has injured Plaintiff and Class Members, had the capacity to injure persons, and has the capacity to injure other persons, and has the capacity to injure persons. Further, its conduct affected the public interest, including the thousands of Washingtonians affected by the Data Breach.

148. As a direct and proximate result of AT&T's unfair methods of competition and unfair or deceptive acts or practices, Plaintiff and Class Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Personal Information.

149. Plaintiff and Class Members seek all monetary and non-monetary relief allowed by law, including actual damages, treble damages, injunctive relief, civil penalties, and attorneys' fees and costs.

VII. REQUEST FOR RELIEF

Plaintiff, individually and on behalf of members of the Nationwide Class and Washington Subclass, as applicable, respectfully requests that the Court enter judgment in Plaintiff's favor and against AT&T, as follows:

KELLER ROHRBACK L.L.P.
1201 Third Avenue, Suite 3400
Seattle, WA 98101-3268
TELEPHONE: (206) 623-1900
FACSIMILE: (206) 623-3384

1. That the Court certify this action as a class action, proper and maintainable pursuant to Rule 23 of the Federal Rules of Civil Procedure; declare that Plaintiff is a proper class representative; and appoint Plaintiff's Counsel as Class Counsel;

2. That the Court grant permanent injunctive relief to prohibit AT&T from continuing to engage in the unlawful acts, omissions, and practices described herein, including;

a. Prohibiting AT&T from engaging in the wrongful and unlawful acts described herein;

b. Requiring AT&T to protect all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

c. Requiring AT&T to delete, destroy and purge the Personal Information of Plaintiff and Class Members unless AT&T can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

d. Requiring AT&T to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of Plaintiff's and Class Members' Personal Information;

e. Requiring AT&T to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on AT&T's systems on a periodic basis, and ordering AT&T to promptly correct any problems or issues detected by such third-party security auditors;

f. Requiring AT&T to engage independent third-party security auditors and internal personnel to run automated security monitoring;

g. Requiring AT&T to audit, test, and train its security personnel regarding any new or modified procedures;

h. Requiring AT&T to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon employees' respective responsibilities with handling Personal Information, as well as protecting the Personal Information of Plaintiff and Class Members;

i. Requiring AT&T to routinely and continually conduct internal training and education, at least annually, to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

KELLER ROHRBACK L.L.P.
1201 Third Avenue, Suite 3400
Seattle, WA 98101-3268
TELEPHONE: (206) 623-1900
FACSIMILE: (206) 623-3384

j. Requiring AT&T to implement a system of testing to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with AT&T's policies, programs and systems for protecting Personal Information;

k. Requiring AT&T to implement, maintain, regularly review and revise as necessary, a threat management program designed to appropriately monitor AT&T's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

l. Requiring AT&T to meaningfully educate all Class Members about the threats they face as a result of the loss of their Personal Information to third parties, as well as the steps affected individuals must take to protect themselves;

m. Requiring AT&T to implement logging and monitoring programs sufficient to track traffic to and from AT&T servers; and

n. Appointing a qualified and independent third-party assessor to conduct for a period of 10 years a SOC 2 Type 2 attestation to evaluate on an annual basis AT&T's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies in compliance with the Court's final judgment.

3. That the Court award Plaintiff and Class and Subclass Members compensatory, consequential, general, and nominal damages in an amount to be determined at trial;

4. That the Court order disgorgement and restitution of all earnings, profits, compensation, and benefits received by AT&T as a result of its unlawful acts, omissions, and practices;

5. That the Court award statutory damages, trebled, and punitive or exemplary damages, to the extent permitted by law;

6. That Plaintiff be granted the declaratory relief sought herein;

7. That the Court award to Plaintiff the costs and disbursements of the action, along with reasonable attorneys' fees, costs, and expenses;

8. That the Court award pre-judgment and post-judgment interest at the maximum legal rate; and

KELLER ROHRBACK L.L.P.
1201 Third Avenue, Suite 3400
Seattle, WA 98101-3268
TELEPHONE: (206) 623-1900
FACSIMILE: (206) 623-3384

9. That the Court grant all such other relief as it deems just and proper.

VIII. DEMAND FOR JURY TRIAL

Plaintiff demands a jury trial on all claims so triable.

RESPECTFULLY SUBMITTED this 18th day of July, 2024.

By: */s Cari Campen Laufenberg*
Cari Campen Laufenberg, WSBA #34354

By: */s Benjamin Gould*
Benjamin Gould, WSBA #44093

KELLER ROHRBACK L.L.P.
1201 Third Avenue, Suite 3400
Seattle, WA 98101-3268
Telephone: (206) 623-1900
Facsimile: (206) 623-3384
claufenberg@kellerrohrback.com
bgould@kellerrohrback.com

Christopher Springer (*pro hac vice forthcoming*)
801Garden Street, Suite 301
Santa Barbara, CA 93101
Telephone: (805) 456-1496
Facsimile: (805) 456-1497
cspringer@kellerrohrback.com

Matthew S. Melamed (*pro hac vice forthcoming*)
180 Grand Avenue, Suite 1380
Oakland, CA 94612
Telephone: (510) 463-3900
Facsimile: (510) 463-3901
mmelamed@kellerrohrback.com

Attorneys for Plaintiff LeDuc Montgomery